Modernized e-File Release 6.1 (MeF 6.1) – Privacy Impact Assessment

PIA Approval Date – October 31, 2008

System Overview

The Modernized e-File, Release 6.1 (MeF 6.1) application allows Transmitters (Trading Partners) to electronically send tax return filings, including accompanying forms, schedules, and attachments. MeF 6.1 accepts submissions for Federal and State returns and stores accepted returns in the Modernized Tax Return Database (M-TRDB). The M–TRDB is a sub-component of MeF 6.1 and is the authoritative system of record for original accepted tax returns that are electronically filed by taxpayers, tax practitioners, and authorized return submitters. Electronic (corporate, partnership, individual, excise, and tax-exempt organization) tax forms are filed through the Internal Revenue Service (IRS) Registered User Portal (RUP).

Systems of Records Notice (SORN):

- IRS 22.062--Electronic Filing Records
- IRS 24.030--Individual Customer Account Database Engine (CADE) Master File
- IRS 50.001--Employee Plans and Exempt Organizations Correspondence Control Records
- IRS 34.037--IRS Audit Trail and Security Records
- IRS 24.046--CADE Individual Master File (IMF) (Formerly: Business Master File (BMF)

Data in the System:

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer – Taxpayer Identification Number (TIN), Name, Address, Date of Birth (DOB), Telephone Number, and Bank Account Number, Routing Transfer Number, amount to debit, and date to debit Taxpayer Dependent's TIN, Name and DOB; and Spouse's TIN, Name and DOB.

B. Employee – During the release, MeF 6.1 will capture and store the employee SEID (not the employee name) on the MeF server. This is for audit continuity purposes, and will be used for no other purpose. No other employee information is captured by MeF.

C. Audit Trail Information – Users can request information from MeF in the EUP (Employee User Port) such as Taxpayer's TIN and Employee's Standard Employee Identifier (SEID), and Name. Information pertaining to each user transaction is captured in the EUP by MeF and forwarded to Security Audit and Analysis System (SAAS). SAAS reports are generated and distributed to the Business Operating Divisions (BODs). The BODs use the reports to monitor employee access. MeF does not generate or distribute the reports. Maintaining the SEID on MeF allows security personnel to trace a transaction from the EUP to MeF. Security operations provide canned and custom reports to BODS/managers. Custom reports are designed after each BOD's needs. Specific IRMs would identify the frequency with which reports would be reviewed.

D. Other – Transmitter's Name, Address, Telephone Number, Electronic Transmitter Identifying Number (ETIN), Electronic Return Originator (ERO) Name, Address, Telephone Number, Electronic Filer Identifying Number (EFIN), Software Developers' Name, Address, Telephone Number, and ETIN.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS:

- MeF obtains the following information from:
  - E-Services – Third Party Data Store (TPDS):
    - Software Developer's:
    - Name
    - Address
    - Telephone Number
    - Software Identification (id) Number
  - Transmitter's
    - Name
    - Address
    - Telephone Number
    - ETIN
  - Electronic Originator (ERO)
    - Name
    - Address
    - ERO Electronic Filer Identifying Number (EFIN)
    - ERO Telephone Number
  - Generalized Mainline Framework (GMF)
    - Employer Identification Number (EIN)
    - Tax Period
    - Filing Type
  - Electronic Filing System (ELF-R)
    - Routing Transit Numbers (RTN)
  - National Accounts Profile (NAP)
    - EIN
    - Name Controls
    - Filing Requirements
  - M–TRDB
    - Taxpayer's (all returns):
      - TIN
      - Name
      - Address
      - DOB
      - Telephone Number
      - Bank account number
      - Routing transfer number
      - Amount to debit account
      - Date to debit account
      - ETIN
      - EFIN
    - 1040 Dependent's:
      - TIN
      - Name
      - Dependent's DOB

- 1040 Spouse's
  - TIN
  - Name
  - DOB
- National Duplicate Tax Identification Number (DUP-TIN)
  - Status Code
  - Message ID number
  - Submission ID number

B. Taxpayer – MeF obtains the following taxpayer return information:
   - TIN
   - Name
   - Address
   - DOB
   - Telephone Number
   - Dependent's TIN
   - Dependent's Name
   - Spouse's TIN
   - Spouse's Name
   - Spouse's DOB
   - Dependent's DOB
   - Bank Account Number
   - ETIN
   - EFIN
   - Software ID number

C. Employee – Beginning in release 6.1, MeF will capture and store the employee SEID (not the employee name) on the MeF server. This is for audit continuity purposes, and will be used for no other purpose. No other employee information is captured by MeF. MeF also forwards the employee's SEID to SAAS for every auditable event in the EUP.

D. Other Third Party Sources – Third party sources are external trading partners which include both software developers and internet filing application users that provide the following information to MeF:
   - Transmitters
     - Name
     - Address
     - Telephone Number
     - ETIN
   - ERO
     - Name
     - Address
     - EFIN
     - ERO Telephone number
   - Software Developer
     - Name
     - Address
     - Telephone Number
     - Software Identification Number (ID)

3. Is each data item required for the business purpose of the system? Explain.
Yes. The taxpayer's information is required for each tax return. The information that is received from other internal IRS systems is used to validate the aforementioned information. The Transmitter and ERO information received from the Transmitter and ERO is matched against the data collected from internal IRS systems.

4. How will each data item be verified for accuracy, timeliness, and completeness?
The back–end portion of MeF validates all tax returns through all methods of transmission against the XML schemas and business rules for IFA and A2A channels Each return prepared and submitted to MeF for e-filing must adhere to the schemas and business rules. If a single data element fails the schema integrity check or business rule failure, the tax return is rejected. Electronic Tax Administration (ETA) supplies the business rules for each return type. MeF enforces the rules against the tax returns using a business rules engine. Business rules enforce relationships between data and forms. When MeF validates returns against the business rules, and if it encounters a discrepancy, the tax return is rejected. The rejected returns remain in the MeF system. They are used by the e–File Help Desk while helping preparer(s) and EROs, understand and fix the errors. MeF accepts current and prior two years' tax returns, but has the functionality to display all returns processed by MeF. New schemas and business rules are issued for each new tax year. Any non–current returns (prior tax years) prepared and submitted must use that year's schema and business rule versions or the returns will fail the schema and business rule validation checks.

5. Is there another source for the data? Explain how that source is or is not used.
No. There is no other source for the data.

6. Generally, how will data be retrieved by the user?
Authorized employees can retrieve and view tax return data using the MeF system's query tools: Return, Request, and Display (RRD) and Help Desk feature. No IRS contractors have access to the data or the tools. Authorized internal users (employees) are System Administrators, Database Administrators, and business users. Internal access is determined by user's job responsibilities and manager's approval. Access is only permitted after a F5081 is submitted with manager's approval, and security, system, and data administrators approve. The 5081 lists the access privileges.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. The following personal identifiers are used to retrieve data:

- Social Security Number (SSN): The SSN is a unique taxpayer Identification number for individuals that can be used to retrieve tax returns of specific taxpayers.
- EIN: The EIN is a unique taxpayer Identification number for businesses that can be used to retrieve tax returns of specific taxpayers.
- Document Locator Number (DLN): A DLN is assigned to each tax return accepted by the MeF system. Each DLN uniquely identifies each tax return of an organization taxpayer. The DLN is used to retrieve a specific tax return for specific taxpayers.
- The ETIN is used to uniquely identify a Transmitter Taxpayer data transmitted by a particular Transmitter. It can be accessed indirectly by querying on that Transmitter's ETIN.
- The EFIN is a number that is used to uniquely identify each ERO. Taxpayer data prepared by a particular ERO can be accessed indirectly by querying on that ERO's EFIN.
- Global Transaction Key (GTX Key): A GTX Key is a number generated that uniquely identifies each transmission and its acknowledgement. Users can view validation results and tax data

contained in an acknowledgement file and transmission file by querying on GTX key. (e–Help Desk personnel and customer service representatives can view acknowledgements and transmission files per role-based access.)
- Submission ID: Submission ID is a number generated by ERO that uniquely identifies tax returns. E–Help Desk personnel will be able to query using the Submission ID.
- Message ID: A Message ID is a number generated by a Transmitter that uniquely identifies a transmission file. E–Help Desk personnel can access tax return data contained in a transmission file by querying on Message ID.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
There are 12 separate user groups within the MeF 6.1 production system. All but four of the user groups are internal to IRS. The remaining four consist of Transmitters, State agencies, Large Taxpayers, and third party software developers. All external user groups could employ contractors. IRS issues ETINs and other external Identifiers or authenticators to external users and their delegates only. All external users and their delegates must pass a suitability investigation. It is the external user's responsibility to protect the data as outlined in numerous publications and IRS rulings.

- Internal Revenue Service employees:

  Role: e-Help Desk Personnel
  Permission: Read Only

  Role: Error Resolution Tax Examiners
  Permission: Read Only

  Role: Examiners
  Permission: Read Only

  Role: Classifiers
  Permission: Read Only

  Role: Accounting
  Permission: Read Only

  Role: Line Managers
  Permission: Read Only

  Role: System Administrator
  Permission: Read/Write/Delete

  Role: Database Administrator
  Permission: Read/Write/Delete

- External Users:

  Role: Transmitters
  Permission: Read/Write

Role: States
Permission: Read/Write

Role: Large Taxpayers
Permission: Read/Write

Role: Software Developers
Permission: Read/Write

9. How is access to the data by a user determined and by whom?
Internal Users (IRS Employees) – Internal Users are subject to management, system administrator, data administrator, and security administrator approval via the Online 5081 (OL5081) system. No contractors have access to the system. OL5081 is used to document access requests, modifications, terminations for all types of users, including system administrators, system accounts requiring Electronic File Transfer Utility (EFTU) access, and test accounts.

External Users – External users apply for access through e-Services. They must pass a suitability background investigation before being given access rights. When they pass the suitability background process, they are provided their ETINS and EFINS. This process is external to MeF.

For external third party and State Trading Partners who access A2A or IFA through the RUP, account registration is performed through e–services and stored within Enterprise Directory and Authentication Services (EDAS). The application process mentioned above determines user's Role Based Access to MeF. Most A2A external trading partners currently use certificate–based authentication. The remaining A2A users are expected to convert to certificate–based authentication in the near future. Those external A2A users not yet using certificate based authentication must use strong-password authentication. A2A password users create their own password. A2A users must enroll their systems using the E–Services Automated Enrollment application. The application uses the user's e-services profile to determine access rights.

Transmitters are given transmitter access and roles but denied State agency roles. State agencies are given State agency access and roles but denied transmitter roles.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.

Yes. Other IRS systems provide, receive, and share data with MeF.

- **NAP** is a compilation of entity data from a number of sources and is used to verify that entity data on tax returns is correct. If a match occurs, MeF continues processing the return. If a match does not occur, MeF rejects the returns.

- **GMF** is a system that is the entry point for pipeline processing. Both electronic and paper returns are input to GMF. MeF sends and receives data to and from GMF. MeF creates one or more extract files that are transmitted to GMF by EFTU. Each extract file contains information on all returns accepted by MeF since the last extract was created. Rejected returns are not extracted and forwarded to MeF. Instead, they remain on the MeF system so that help desk assistors may access them to assist preparers perfecting the rejected returns. All data transfer sessions between MeF and GMF are done by EFTU and are encrypted.

- **National Duplicate Tax Identification Number (DUP–TIN):** The DUP–TIN database houses all SSNs contained on all filed 1040 tax returns for the current tax filing year. After NAP completes its validation checks on return data received from MeF, if there are no validation errors it inserts the SSNs from the return into the DUP–TIN database, if none of the SSNs already exist in the database. All sessions between MeF and DUP–TIN are SSL encrypted and use certificate–based authentication between systems.

- **E-Services – Third Party Data Store (TPDS)** is an application module of the E-Services application. MeF Receives and sends data to and from E-Services. MeF receives extract files from E-Services by way of EFTU. These files contain information on transmitters, EROs, and approved software tax preparation packages and are loaded into the MeF database. The Transmitter data includes Transmitter ETIN, address, point of contact, and phone number. The ERO data includes ERO EFIN, address, point of contact, and phone number. The approved software extract contains the package's software ID and return type, and it is approved by E–File. No tax return data is included in these extracts. MeF also sends statistical information about tax returns, transmitters, EROs, software packages to E-Service by way of EFTU. The data includes ETINs, EFIN, and software IDs, but no taxpayer entity data. This data is used in reports by E-Services. All EFTU transmission sessions between E–Services and MeF are encrypted.

- **Electronic Federal Payment Posting System (EFPPS)** – MeF sends data to EFPPS to debit taxpayer's accounts for those taxpayers who indicate on their return they want to make an electronic payment. Taxpayers who make an electronic payment attach a payment voucher to their return. If MeF accepts the return, it converts the voucher information into EFPPS format. The data includes taxpayer TIN, bank account, amount to debit, date to debit, and bank routing transfer number. This data is forwarded to EFPPS in daily extracts through EFTU. The transfer sessions between MeF, EFTU, and EFPPS are encrypted.

- **Electronic Tax Administration Research and Analysis System (ETARAS)** was created to give e–file program owners, managers, and executives information about electronic filing. Currently, ETARAS contains data on electronically transmitted business and individual (1040 series) tax returns, Transmitters and Electronic Originators, refunds, and payment information. The transfer sessions between MeF, EFTU, and the ETARAS systems are encrypted.

- **E–File Reports** is a system that serves as a repository for all IMF electronic filing return statistics. MeF sends statistical and summary data about 1040 filings to the E–File Reports system. Examples of the type of information sent includes number of Federal filings by day and by State, the amount collected each day, and the number of State returns filed each day. No taxpayer entity data is sent to the E–File Reports system.

- **Integrated Data Retrieval System – End of Day (IDRS–EOD)** is an application module of the Modernization & Information Technology Services (MITS) owned IDRS application. The IDRS is a major application supported under the Service Center Support Systems (SCSS). The data captured includes parent TIN, subsidiary TINs, tax type, and tax years. Upon receiving this information, EOD satisfies the subsidiaries' filing requirements and transfers any credits from its accounts to the parents. The transfer sessions between MeF, EFTU, and EOD are encrypted using SFTP.

- **Electronic Tax Administration Marketing Database (ETA MDB)** is a market research database developed to support the overall ETA marketing effort of expanding each annual campaign for informing and educating taxpayers and practitioners about the benefits of electronic filing.

- **Excise Tax E–file and Compliance (ETEC) Vehicle Identification Number (VIN) Datastore (MITS–18)** is considered part of the MITS-18 General Support System (GSS) boundary. MeF receives and processes excise tax submissions and claims including the Form 2290 – Heavy Highway Vehicle Use Tax. MeF extracts VIN data from an accepted 2290 submission and sends messages containing VIN data to the ETEC System via transactional messaging. The data includes the taxpayer's EIN.

- **Control–D WebAccess** servers will be used to pass-through to the Integrated Collection System/Automated Collection System/Print (IAP) mainframes Control–D repository for viewing and printing reports that are stored on the IAP Mainframes. Control–D WebAccess is a technological enhancement that will significantly reduce the amount of printed output.

- **Tax Return Data Base (TRDB)** – Taxpayers call Customer Service Toll Free seeking assistance correcting e–filed 1040 returns that have been rejected by the IRS e–file system. To assist these taxpayers, Customer Service employees access TRDB to view the reasons why the return was rejected. Since Customer Service does not have access to MeF RRD, information about 1040 returns rejected by MeF have to be provided to TRDB. Therefore, MeF converts 1040 reject information, including error messages, into TRDB format, and then transports that data to TRDB.

- **Modernized Tax Return Database (M–TRDB)** – M–TRDB is the authoritative source of all tax returns accepted by MeF. Accepted returns (pass schema and business rule validation) are inserted into M–TRDB. Rejected returns remain in MeF database. When RRD users request accepted return information, MeF retrieves from M–TRDB and returns the data to the requesting users. M–TRDB also provides extracts of accepted return data to various downstream internal IRS systems.

- **Electronic Filing System (ELF–R)** – ELF–R manages 1040 tax returns received electronically from preparers or telephonically from individual taxpayers and passes accepted information to GMF. It is used to view electronically filed 1040s for older tax years. MeF receives one file from ELF once a quarter via EFTU, and the session is encrypted using SFTP. That file contains the list of Routing Transit Numbers (RTNs). The extract is loaded into the MeF database, and as returns are processed if the payment voucher is attached, MeF validates the RTN in the voucher against the list of valid RTNs in that extract.

- **Large and Mid-Size Business (LMSB) Data Capture System (DCS)** –The LMSB DCS provides LMSB with the Taxpayer Registry derived from taxpayer filings including, but not limited to, the Corporate Tax Return form 1120 and the entire 1120 family of returns, Partnership returns form 1065, Sub–Chapter S Corporation return form 1120S, and supporting tax return schedules such as forms K–1 Partners Distributive Shares of Partnership Interest, 851 Corporate Affiliations Schedule, and forms 5471 and 5472 for international affiliations.

- **Political Organization Filing and Disclosure and 527 Political Action Committee (527 PAC/POFD) – E–Postcard Public Disclosure (MITS–28)** collects, validates and stores information from IRS forms 8871, 8872, and 990. The functionality of this system is required by

law to provide political organizations the ability to identify their status and report contributions and expenditures. Information collected from political organizations is required to be made available to the general public. E–Postcard Public Disclosure allows users to retrieve, display or download Form 990–N filings (ePostcards).

- **Statistics of Income Distributed Processing System (SOI–DPS)** includes databases, applications, and scanning required supporting the Service's requirement to report to Congress annually on the numbers and types of returns filed, the characteristics of those returns, and the money amounts reported on those returns. SOI–DPS is designed to facilitate the collection, production and publication of statistical data for use in the formulation and measurement of legislation relating to taxation as required under Internal Revenue Code (IRC) 6108. SOI utilizes data sources to perfect data for statistical purposes. The data is based on individual, corporate, partnership, exempt organization, and estate tax returns, plus those related to foreign activities. Public Access System (PAS) is system that is responsible for the public display of form 990, 990–N, 990-PF, and 990–EZ.

- **Integrated Production Model (IPM) – XRDB Extract** is a common, read-only data store containing core IRS data. (e.g., tax accounts, tax returns, and information. The purpose of the IPM is to provide one central relational database populated with current and historical data. The consolidation of data sources into a centralized data store provides a single point of access to corporate data.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Yes.

National Accounts Profile (NAP**)**
- Authorization to Operate (ATO) – February 13, 2009
- Privacy Impact Assessment (PIA) – December 1, 2008

Generalized Mainline Framework (GMF)
- Authorization to Operate (ATO) – February 18, 2009
- Privacy Impact Assessment (PIA) – October 16, 2008

Duplicate Tax Identification Number (DUP–TIN)
- Authorization to Operate (ATO) – Non–App
- Privacy Impact Assessment (PIA) – Non–App

E-Services
- Authorization to Operate (ATO) – April 2, 2008
- Privacy Impact Assessment (PIA) – December 17, 2007

Electronic Federal Payment Posting System (EFPPS)
- Authorization to Operate (ATO) – April 3, 2007 (formally EFTPS)
- Privacy Impact Assessment (PIA) – (formally EFTPS–Approval memo dated April 27, 2009.)

Electronic Tax Administration Research and Analysis System (ETARAS)
- Authorization to Operate (ATO) – May 18, 2007
- Privacy Impact Assessment (PIA) – May 26, 2007

E-File Report
- Authorization to Operate (ATO) – April 30, 2009
- Privacy Impact Assessment (PIA) – February 27, 2009

Integrated Data Retrieval System – End of Day (IDRS-EOD)
- Authorization to Operate (ATO) – March 10, 2009
- Privacy Impact Assessment (PIA) – May 20, 2009

Electronic Tax Administration Marketing Database (ETA MDB)
- Authorization to Operate (ATO) – May 22, 2009
- Privacy Impact Assessment (PIA) – December 23, 2008

Excise Tax E-file and Compliance (ETEC) Vehicle Identification Number (VIN) Datastore (MITS–18)
- Authorization to Operate (ATO) – June 2, 2008
- Privacy Impact Assessment (PIA) – Not Applicable (Qualifying Questionnaire May 1, 2007)

Control-D WebAccess
- Authorization to Operate (ATO) – (Not a FISMA reporting system)
- Privacy Impact Assessment (PIA) – (Not a FISMA reporting system)

Tax Return Data Base (TRDB)
- Authorization to Operate (ATO) – May 18, 2007
- Privacy Impact Assessment (PIA) – (MCD) – April 13, 2009

Modernized Tax Return Database (M–TRDB)
- Authorization to Operate (ATO) – May 9, 2007
- Privacy Impact Assessment (PIA) – Not applicable

Electronic Filing System (ELF-R)
- Authorization to Operate (ATO) – May 26, 2009
- Privacy Impact Assessment (PIA) – April 19, 2009

Data Capture System (DCS)
- Authorization to Operate (ATO) – October 29, 2007
- Privacy Impact Assessment (PIA) – November 7, 2007

Political Organization Filing and Disclosure and 527 Political Action Committee (527 PAC/POFD) E–Postcard Public Disclosure
- Authorization to Operate (ATO) – June 2, 2008
- Privacy Impact Assessment (PIA) – September 7, 2009

Statistics of Income Distributed Processing System (SOI–DPS)
- Authorization to Operate (ATO) – June 30, 2008
- Privacy Impact Assessment (PIA) – April 4, 2008

Integrated Production Model (IPM)
- Authorization to Operate (ATO) – August 4, 2008
- Privacy Impact Assessment (PIA) – September 12, 2008

12. Will other agencies provide, receive, or share data in any form with this system?
Yes, States. State Taxing Authorities (listed as one of the external users in item #8 above) retrieve State returns from the MeF application that were submitted by Transmitters. Once the State has been accepted as an Authorized IRS e–file user, they are issued an ETIN. Once an ETIN is issued, they may retrieve State returns.

In addition to the ETIN, any transmitter or State agency using the A2A services must also obtain an application system ID from the IRS, and provide this ID in each service request. State agencies can retrieve their State submissions from, and forward their State-generated acknowledgements to MeF. To do this, each State agency must register with the IRS. The IRS will issue an ETIN to each registered State, just as it issues one for each registered Transmitter. If a State agency is not registered, the agency cannot access MeF.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
At the end of the retention period, data will be purged from the MeF system according to standard IRS procedures – Internal Revenue Manual (IRM) 1.15.29 – Records Control Schedule for Submissions Processing Campus Records.

- 55 – Electronically Filed Individual, Partnership and Fiduciary Income Tax Returns – (a) Destroy on or after January 16, six years after the end of the processing year unless needed for Collection Statute Expiration Date Extract due to a balance due.

- 58 – U.S. Corporation Income Tax Return – (b) Destroy 75 years after end of the processing year.

- 66 – Exempt Organization Returns – (b) Destroy 6 years after the end of the processing year.

- 67– Miscellaneous Tax Returns – (b) Destroy 6 years after the end of the processing year.

- 68 – Extension Records – (a) Destroy 1 year after end of processing year.

- 82 – Heavy Vehicle Use Tax Return – (b) Destroy 6 years after the end of the processing year.

- 84 – Taxpayer Application for a change in Accounting Period, and Application for Change in Accounting Method (Forms 8716 and 3115) – (b) Destroy 4 years after end of processing year.

- 85 – Information Returns – (1) Domestic Filed – (a) Associated with income tax returns-(a) Destroy when related income tax returns are destroyed or retired.

- 85 – Information Returns – (c) Statement of Gambling Winnings and Transmittal (Form 1099R) – (a) Destroy 3 years after processing year.

- 85 – Information Returns – (2) Foreign Filed – (a) Associated with income tax returns – (a) Destroy when related income tax returns are destroyed or retired.

- 107 – Form 8697, Interest Computation Under Lookback Method for Computing Long Term Contract. (b) Destroy 5 years after end of processing year.

- 344 – Information Return with Respect to a Foreign Corporation (Form 5471) – (b) Destroy 5 years after end of processing year.

- 345 – Information Return of a Foreign Owned Corporation (Form 5472)-(b) Destroy 5 years after end of processing year.

14. Will this system use technology in a new way?
No. MeF will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
No. MeF is not designed to identify, track, locate, or monitor individuals and will not be used for any identification purposes. MeF is designed to process e-filed tax returns for individuals and organizations.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
No. MeF is not designed to identify, locate, and monitor groups of people.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. Taxpayer or group of taxpayers are not treated differently from any other taxpayer of group of taxpayers. All tax returns must adhere to the same rules. There are no exceptions.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Not Applicable. MeF does not make any determination (positive or negative) on filed tax returns.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
Yes. Cookies and Security Access Mark-up Language (SAML) persist for the duration of a session (re–authentication) but not across sessions.

View other PIAs on IRS.gov